PATENT ABSTRACTS OF JAPAN

(11)Publication number : **09-233541**

(43)Date of publication of application : **05.09.1997**

(51)Int.Cl. **H04Q 7/38**

(21)Application number : **09-030494**

(22)Date of filing : **14.02.1997**

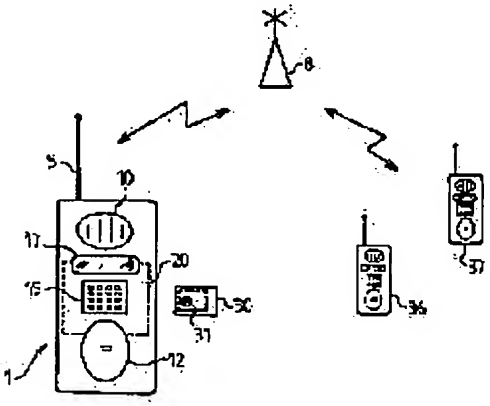
(71)Applicant : **PHILIPS ELECTRON NV**

(72)Inventor : **GASPARINI STEPHANE**
GEFFROTIN BERNARD

(30)Priority

Priority number : **96 9601815** Priority date : **14.02.1996** Priority country : **FR**

(54) TRANSMISSION SYSTEM HAVING TERMINAL EQUIPMENT PROVIDED WITH PREPAID CIRCUIT



(57)Abstract:

PROBLEM TO BE SOLVED: To provide a connectable circuit formed from an SIM card having no demerit that damage such as changing contents through illegal trick is easily received.

SOLUTION: This transmission system has plural terminal equipments 1, 36 and 37 respectively provided with one connectable circuit 30 storing prepaid data at least. The terminal equipment 1, 36 and 37 is provided with a means for directly changing these prepaid data corresponding to communication. Further, a protecting means is provided for protecting these data concerning this prepaid state. Thus, a prepaid card can be used for a GSM network or any similar network.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

A09-233541

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] It is the transmission system characterized by to include the protection means for guaranteeing the data integrity concerning [on the transmission system which has two or more terminal units which can perform the communication link including the circuit where prepayment data are contained in it, and in which at least one connection is possible, and a means to change the above-mentioned prepayment data directly according to a communication link, and / the above-mentioned terminal unit] prepayment.

[Claim 2] a transmission system including the relay center which interconnects a terminal unit according to claim 1 -- setting -- accounting -- a rate -- the transmission system characterized by defining data on the level of the above-mentioned relay center.

[Claim 3] a transmission system according to claim 1 -- setting -- accounting -- a rate -- the transmission system characterized by defining data on the table contained in memory on the level of each terminal unit.

[Claim 4] It is the transmission system characterized by being formed by the detection means for the above-mentioned protection means detecting the above-mentioned employment data integrity in the transmission system which operates gaining assistance of the employment data with which the terminal unit given in claim 1 thru/or any 1 term of 3 is memorized in memory.

[Claim 5] It is the transmission system characterized by being formed by authentication means to attest a terminal unit through the circuit in which the connection for permitting a communication link when it is admitted in a transmission system given in claim 1 thru/or any 1 term of 4 that the above-mentioned protection means is Shinsei is possible.

[Claim 6] It is the transmission system characterized by being formed by the protection means for the above-mentioned protection means protecting the data exchange between a terminal unit and a connectable circuit in a transmission system given in claim 1 thru/or any 1 term of 5.

[Claim 7] It is the terminal unit characterized by to include the protection means for guaranteeing the data integrity concerning [on the terminal unit for which the communication link including the circuit where the prepayment data about a communication link are contained in it, and in which at least one connection is possible, and a means to change the above-mentioned prepayment data directly as a communicative function is exchangeable, and / this terminal unit] prepayment.

[Claim 8] It is the terminal unit characterized by being formed by the detection means for the above-mentioned protection means detecting the above-mentioned employment data integrity in the terminal unit in which the actuation becomes settled with the employment data memorized in memory according to claim 7.

[Claim 9] It is the terminal unit characterized by being formed by authentication means to attest a terminal unit through the connectable circuit which permits a communication link when it is admitted in a terminal unit according to claim 7 or 8 that the above-mentioned protection means is Shinsei.

[Claim 10] It is the terminal unit characterized by being formed by the protection means for the above-mentioned protection means protecting the data exchange between a terminal unit and a connectable circuit in a terminal unit given in claim 7 thru/or any 1 term of 9.

[Claim 11] This approach is each next phase, i.e., :-, setting the actuation including the prepayment data which specify a certain fixed balance to the prepayment approach for transmission systems of having two or more terminal units which the connectable prepayment circuit specified by software has combined with it by plug insertion. The

beginning phase which checks the integrity of the software of a terminal unit of operation, and checks the connectable type of a prepayment circuit;
- Sending-out phase sent out to the prepayment circuit which can connect the key from a terminal unit;
- Connection setting phase in comparison with the minimum tariff which should charge the balance contained in a connectable prepayment circuit;
- the rate under communication link which performs pulling down from the contents of the balance -- the prepayment approach characterized by having accounting phase; and changing.
[Claim 12] It is the prepayment approach characterized by being that from which prepayment data are periodically pulled down in a certain pulling-down unit in the prepayment approach according to claim 11.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the transmission system which has two or more terminal units which can perform the communication link including the circuit where prepayment data are contained in it, and in which at least one connection is possible, and a means to change the above-mentioned prepayment data directly according to a communication link.
[0002] This invention relates also to the prepayment approach performed again with the terminal unit suitable for an above-mentioned system and such an above-mentioned system.
[0003]
[Description of the Prior Art] This kind The radical Motohara rule of the network of a GSM mold is spreading all above-mentioned equipments generally widely first. And it is in a general target. A SIM card or micro Using the connectable circuit formed with the chip called a SIM card, it is made the thing for each people to a user, and equipment is **. A SIM card or micro Once a SIM card is inserted in a terminal unit with a plug, it permits carrying out an identification check and attesting a user to a network.
[0004] Commercial company who contracts management of a subscriber for a network management person's profits (SCS) It joins. A SIM card can come to hand. Not only subscription business but SCS also manages claim business based on the data sent by the network management person.
[0005] Such management business is comparatively expensive. Not only it but the risk on financial affairs cannot be disregarded, namely, :some people's subscriber is that of "forgetting or neglecting" about paying for the bill.
[0006] It reaches a network management person for these reasons. SCS is interested in installation of the prepayment network service according to the idea of the telephone card used by the public telephone booth today. Prepayment type A SIM card permits the communication link corresponding to the total number of units, or the number of predetermined units. : from which this concept also hangs down the following various advantages - Simplification [of the distribution process of a SIM card];
- Increment in a subscriber number of registration;
- Bill issue is needlessness.;
- Reduction of management costs;
- Progressive source of revenue.
[0007] the above prepayment systems -- the [PCT patent record] -- it is known from WO 95/No. 28062. However, a means by which it may be intercepted by those to whom this system has a remarkable fault, I hear that a connectable circuit tends to suffer damage, and it has it, the contents may be changed into by the unjust artifice, and exchange of the data between this circuit and terminal unit has malice, and it means unjust action is offered.
[0008]
[Problem(s) to be Solved by the Invention] This invention proposes the system of the type of a publication at the beginning which does not have an above-mentioned fault at least.
[0009]
[Means for Solving the Problem] Therefore, the system of a type given in the beginning is characterized by including

a protection means for the above-mentioned terminal unit guaranteeing the data integrity about prepayment.

[0010] This invention-idea consists of all the information about prepayment data being protected and those who plan injustice by it making impossible the activation top of deceiving that communication link cost.

[0011] One mode of this invention by the system of the above-mentioned type on which a terminal unit functions gaining assistance of the employment data memorized by memory is characterized by being formed by the detection means for the above-mentioned protection means detecting the above-mentioned employment data integrity, and this mode is not certainly changed by those to whom those data mean injustice.

[0012] According to another mode of this invention, the above-mentioned protection means is formed by means to attest a terminal unit in the circuit in which the connection for permitting a communication link is possible, when being Shinsei is admitted, and those who plan injustice avoid possibility of plug connection of the circuit in which other connection is possible being made, and aiming at profits to him about communication link cost.

[0013]

[Example] Hereafter, the above of this invention and other modes are explained to a detail by an example and the drawing.

[0014] The system shown in drawing 1 contains what attached 1 and a number with the pocket form wireless terminal unit. This equipment It has the antenna 5 for sending and receiving an electric wave between the relay centers 8 of the wireless network of a GSM mold. This equipment 1 includes a loud speaker 10, a microphone 12, a keypad 15, and the visible display 17. Having surrounded with the broken line expresses the electronic part 20 in this equipment. According to the GSM criterion (I-ETS 300 045-1 or ETS30), they are an ISO format or a plug-in format. A SIM card or micro A SIM card is prepared and, as for this, 30 and a number are attached by drawing 1 . This card has a connector 31 and it contacts another [which forms some equipments 1] contact 35. Another [this] contact 35 is shown in drawing 2 . Equipment 1 and other equipments 36 and 37 of the same structure are further contained in the system of drawing 1 .

[0015] The structure of equipment 1 is further shown in a detail at drawing 2 , and the same number as what has the same drawing 1 and the same drawing 2 is attached. Drawing 2 shows the structure of the electronic part 20 to a detail.

[0016] This electronic part 20 The transmitting assembly 40 and the receiving assembly 42 for sending and receiving the various data usually used with a GSM technique, the data which will come from a microphone 12 if it says in more detail, and the data about a loud speaker 10 are included. The microprocessor assembly 50 is the receiving assembly 42 in many following elements, i.e., :transmitting assembly 40 list, Keypad 15, Visible display 17, And management of data-exchange; of module SIM 30 is guaranteed to connector 35 list through 31. Furthermore, if it says in detail, this microprocessor assembly 50 will be. An EPROM mold is made suitable and it has read-out / write-in memory 55 which means that prepayment data are included in it.

[0017] If this system is based on this invention Accounting to a communication link is wanted to come to allow through a SIM card.

[0018] therefore, such a system -- following requirements: - - to which a SIM card can fail (accuracy of accounting count) to subtract only the amount of money corresponding to the offered service the ** by which the unit to which a user corresponds dropping [lengthen] is not made -- service -- it cannot receive (with no unauthorized use) -- it is made satisfied Radical Motohara ** of this invention: - A SIM card has what can perform re-payment, and the thing which is not made, when it is paid in advance per unit and the balance is used up.;

- Terminal unit It charges by the rate of a SIM card.;

- To the terminal unit which can charge a card on a network Only when a SIM card is inserted A SIM card can be used.;

- A terminal unit contains the application of an algorithm required for the prepayment in the processor which guarantees activation of the software function of a terminal unit and which was left in trust, and the environment where it protected.;

- The processor left in trust can forbid operation actuation, when the integrity of the software of a terminal unit can be checked and it is changed.;

- A code protocol is a terminal unit. It permits establishing the link where it was entrusted between SIM cards.;

- It protects in code to forgery of arbitration. The original balance of a SIM card is read by the terminal unit.;

: Terminal unit It can guarantee that it is the true exact fruit of the balance of a SIM card, and, in the case of insufficient funds, a communication link can be forbidden.;

- Terminal unit It which calculates the rate of SIM shall be based on the data with which it was based on the rate data of phonecall charges sent from a network at the beginning of communicative, or the form of a table was initialized beforehand.;

- Terminal unit the rate by which the address is carried out to a SIM card --; from which directions are protected in code to forgery of arbitration

- The rate of a SIM card is protected in code to forgery of arbitration. It can check through the balance of a SIM card.;

- Processor to which the terminal unit was entrusted The code exact private seal of the effective rate of SIM is guaranteed.;

- Terminal unit A communication link is cut when the balance of a SIM card is used up.

[0019] Drawing 3 and the drawing after it are drawings showing operation actuation of the system to which the above-mentioned requirements are satisfied.

[0020] Operation actuation is divided at four phases expressed with the flow chart shown in drawing 3 and the drawing after it, respectively. these flow charts -- the following two parts, i.e., :, - Partial; named TERM about operation actuation of a terminal unit 1, and - It is related with SIM card 30. It is formed of partial; named SMC.

[0021] This step K0 from which the phase shown in drawing 3 begins at step K0 is a step which supplies a power source to a terminal unit, and the operation of the following beginning consists of checking the integrity of the software of a terminal unit (step K2 reference). It is French patent ****** for which the applicant same about this as this application applied on February 7, 1996. It is indicated by 96 01 478 No. By the next trial (step K5), if it is shown that software is invaded, it will progress to step K6 and a halt of a terminal unit 1 will be directed. Supposing software is unhurt It is guaranteed that operation actuation of the terminal unit by the SIM card is attested, and management of the rate of a communication link unit can do a terminal unit., This is performed by challenge/response mechanism.

[0022] It is an initiation instruction because of this purpose. (step K10) It is given to SIM card 30. Then, ** A SIM card starts (step L0). ** After SIM starts, a terminal unit is step K12. Request of a random number It sends out to a SIM card. ** SIM answers by receiving the request and generating a random number As (step L2). A terminal unit works through Key Ks and the encryption algorithm concerning several S, and is this algorithm. It is sent out to a SIM card. (step K14) . This card answers several S received and performs an operation. This operation is prescribed by the encryption algorithm described as Ag (Kv, S) into step L4. This algorithm If the RSA coding approach is included, two keys Ks and Kv will be used. these keys -- if -- a symmetrical approach like the DES approach is used -- it is the same if it becomes. Next, they are two numbers As and As' at step L6. It is compared. If this comparison shows a difference, a process will stop (step L8). A card is blocked until it starts next time.

[0023] the following step -- traditional -- network ; which consists of making SIM attest -- this is called A3 A8 (indicated by the GSM criterion) An algorithm is used. the standard standard procedure for GSM -- it is -- step L10 **** -- this -- AgA three A8 (..) -- writing -- **** -- ** It is the key Ki of SIM. If Authentication of the terminal unit by the SIM card is completed correctly, and if there is nothing, it will call at a network. It is unrealizable, consequently processing of recognition of SIM is a network. It will be understood that connection of this handset that cannot perform pulling down SIM will be refused. Therefore, a terminal unit is delivery to a card about a random number Ar. (step K18) Then, a card calculates several R as the function of A3A8 algorithm, and a function of Key Ki as mentioned above. This number is sent out to a terminal unit and is further sent on a network. (step K20) . It is judged [by which the terminal unit has been received, for example / or or] on the level of a relay center 8 whether refusal was carried out.

[0024] The 2nd phase shown in drawing 4 is a terminal unit. It is the phase which establishes the random session key which means protecting exchange between SIM cards. A terminal unit generates the random session key Ks. (step K30) . Encryption of this key is performed with the algorithm of a RSA mold. (step K32) . Request whose key Kenc generates a session key It is used for asking for the message C sent out to SIM. (step K33) . SIM card The key Ks which decoded and asked for Message C using an RSA algorithm and its key Kdec is memorized.

notes: - the layout of this and the equivalent -- for example, -- Based on the algorithm of symmetry like a DES algorithm, it is possible. In that case, Key Kenc and Key Kdec will become the same thing.

[0025] another deformation of activation of a symmetry algorithm -- for example, -- a DES algorithm -- terminal unit It consists of using the random number given by the known key of a SIM card, and two existing parts. A terminal unit generates a random number Am and memorizes it. It sends out to a SIM card. A SIM card generates a random number As and sends it out to a terminal unit, and Ks-Ag (Key, As| |Am) is calculated, it is memorized, and a terminal unit specifies a logic chain operation further again. A terminal unit also calculates Ks=Ag (Key, As| |Am) further to them, after receiving As to it and coincidence.

[0026] In the exchange, the terminal unit beforehand known for the way with few artful extent reaches. The key Ks of a SIM card can also be used.

[0027] The 3rd phase is a phase which takes asking for a communicative parameter into consideration, and it checks whether it is enough to the communication link by which the balance of the unit on a card is established. This phase is explained by drawing 5 .

[0028] after starting a communication link (step K40) communication link accounting -- the parameter of a rate is called for based on the table beforehand carried in the network operator or the terminal unit. This is step K42. It is shown. Subsequently, approach Prd It is started and this permits recovery of the balance of the card with which the guarantee of all security was made. When, as for this approach, a random number Ac is generated (step K44) Starting, this random number Ac is Balance Sld. It is added to the receiving request. (step K46) . If it does so A SIM card is based on a numeric value Ac. It is :m1 = AlgD, however (Ac, Ks) ** which calculate the certificate and the balance which are called MAC in the following way, and Ks is taken as the session key established before.;

m2 = AlgD (balance (+) m1, Ks)

however, **, (+) a operator called an exclusive OR (EXCLUSIVE-OR) is expressed -- AlgD If the algorithm of arbitration is further specified in this case the result which expresses a DES algorithm and forms Ms = MAC -- m2 It becomes four leftmost digit cutting tools. This is step L30. It is expressed. next -- a SIM card -- a random number Ad -- generating -- (step L32) this -- after -- a rate -- it is used for a request. And finally a card sends out Sld (balance), Ms, and the new random number Ad to a terminal unit. (step L33) . The balance and Ms If it receives, a terminal unit is based on the numeric values Ac and Ks to which the integrity was established by the next re-calculation, and it established :m1'= AlgD (Ac, Ks) by itself, and is;m2'= AlgD (balance (+) m1, Ks). It checks by doing; re-calculation of based on the balance which SIM sent out. It becomes four leftmost digit cutting tools of Ms'=m2'. This is step K48. It is expressed. Subsequently, step K50 Ms' and Ms Equivalence is examined. When it was equivalence, it received. The integrity of the value of the balance of SIM is proved. If it is not equivalence, a communication link will be interrupted in that case. (step K51) . This actually has the suppression effectiveness that an unjust intention makes communicative establishment impossible as a result. To a degree (step K52) The rate Db by which it is charged is step K42. It is calculated based on the received parameter. this balance Db and the minimum -- comparison with a rate (step K54) The judgment of whether to make a communication link establish can be performed. If a communication link is interrupted, it will be step K55. It goes. If a communication link is continued, it will go to step K56, and allocation of Variable OSLD is directed there. It is made for this variable to have included the numeric value of the balance which comes from a card. terminal unit the random number Ad received from SIM -- memorizing -- a next rate -- it uses as well as a request.

[0029] The flow chart of the 4th phase is shown in drawing 6 , and this shows the rate charged during a communication link at a card. this phase -- a certain accounting -- it starts at the moment of a rate being charged (step K60) . this initiation -- for example, -- periodic -- a rate -- it is made by the terminal unit which it is going to make Unit Db charge. An accounting operation is step K62. Certificate explained (one MAC) It protects. Subsequently, the request to a rate is sent to a SIM card. (step K64) . There, certificate Md' is defined based on the selected key Ks (step L50). (step L51) Certificate Md with which it was sent out from the terminal unit It is compared. (step L55) . If the result of a comparison is good, it is step L60. It progresses and operation actuation of the new balance is directed there. It is appropriate to check that this new balance is the number of pluses, and it is step L62. It performs. A card is blocked if the balance is the number of minus. (step L63) . Any operation will not be performed, either, if the balance is the number of pluses. This card is declared to be O.K. (step L65) It is sent out to a terminal unit.

[0030] A terminal unit is this declaration when it does so. (step K65) It is ** by examining. It is possible to check whether a SIM card is effective. If If the SIM card is blocked, since it is not declared as O.K., a communication link stops. (step K66) . If It is Approach Prd if a SIM card is effective. By performing, a process is continued and recovery

of a balance value is permitted. The check of a true rate is performed. (step K70) Variable OSLD is step K75. It is updated. If a check shows that a rate is not carried out, a communication link will stop. (step K71) .

[0031] This invention It will be applied also to the terminal unit used in the environment where an application field is found out by **, such as fields other than the network of a GSM mold especially a telephone network, the data transmission network of DCS 1800 type, mount or a fixed-line telephone terminal unit (coin box set), facsimile, data, or a picture transmission terminal unit, and neither protection nor a monitor is carried out.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] Drawing 1 is drawing showing the system by this invention.

[Drawing 2] Drawing 2 is drawing showing the pocket form wireless terminal unit suitable for the system shown in drawing 1 .

[Drawing 3] Drawing 3 is drawing showing the 1st flow chart which meant explaining operation actuation of the system by this invention.

[Drawing 4] Drawing 4 is drawing showing the 2nd flow chart which meant explaining operation actuation of the system by this invention.

[Drawing 5] Drawing 5 is drawing showing the 3rd flow chart which meant explaining operation actuation of the system by this invention.

[Drawing 6] Drawing 6 is drawing showing the 4th flow chart which meant explaining operation actuation of the system by this invention.

[Description of Notations]

1 Pocket Form Wireless Terminal Unit
5 Antenna
8 Relay Center of Wireless Network
10 Loud Speaker
12 Microphone
15 Keypad
17 Visible Display
20 Electronic Part in Pocket Form Wireless Terminal Unit
30 SIM Card
40 Transmitting Assembly
42 Receiving Assembly
50 Microprocessor Assembly
55 Read-out / Write-in Memory

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－233541

(43)公開日　平成９年(1997)９月５日

(51)Int.Cl.[6]	識別記号	庁内整理番号	Ｆ Ｉ		技術表示箇所
Ｈ０４Ｑ　7/38			Ｈ０４Ｂ　7/26	１０９Ｊ	

審査請求　未請求　請求項の数12　ＯＬ　（全 ７ 頁）

(21)出願番号　特願平9－30494

(22)出願日　平成９年(1997)２月14日

(31)優先権主張番号　９６０１８１５

(32)優先日　1996年２月14日

(33)優先権主張国　フランス（ＦＲ）

(71)出願人　590000248
フィリップス　エレクトロニクス　ネムローゼ　フェンノートシャップ
PHILIPS ELECTRONICS N. V.
オランダ国　アインドーフェン　フルーネヴァウツウエッハ　1

(72)発明者　ステファーヌ　ガスパリニ
フランス国　72700　アロンヌ　リュ　ダロンヌ　14

(72)発明者　ベルナール　ゲフロタン
フランス国　92190　ムドン　ビ　シュマン　デ　サン　クロード　5

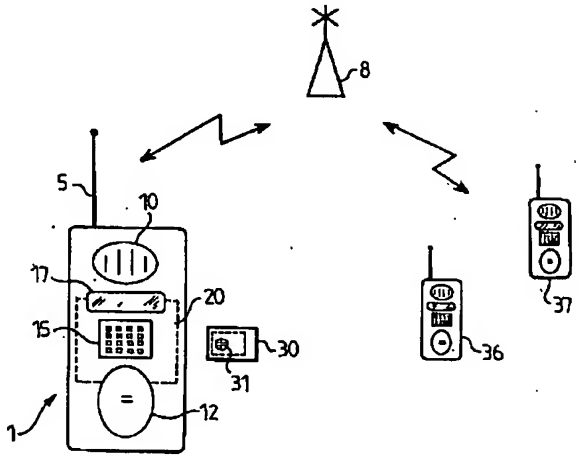
(74)代理人　弁理士　杉村　暁秀　（外３名）

(54)【発明の名称】　前払い回路を含む端末装置を有する伝送システム

(57)【要約】

【課題】　不正な策略により内容が変更される等の被害を受け易い、という欠点を持たない SIMカードで形成される接続可能な回路の提供。

【解決手段】　この伝送システムはその中に前払いデータが入っている少なくとも１つの接続可能な回路(30)を含む複数の端末装置(1,36,37) を有する。該端末装置(1,36,37) は通信に応じて上記前払いデータを直接変更する手段を含む。更にこの前払いに関しこれらのデータを防護するための防護手段が設けられている。このようにしてGSM ネットワーク又は類似のネットワークにおいて前払いカードが使用できる。



1

【特許請求の範囲】

【請求項１】　その中に前払いデータが入っている少なくとも１つの接続可能な回路と、通信に応じて上記前払いデータを直接変更する手段とを含むところの、通信を行うことのできる複数の端末装置を有する伝送システムにおいて、

上記端末装置は前払いに関するデータの完全性を保証するための防護手段を含むことを特徴とする伝送システム。

【請求項２】　請求項１に記載の、端末装置を相互接続する中継局を含む伝送システムにおいて、課金料率データは上記中継局のレベルで定められることを特徴とする伝送システム。

【請求項３】　請求項１に記載の伝送システムにおいて、課金料率データは各端末装置のレベルでメモリに含まれているテーブルによって定められることを特徴とする伝送システム。

【請求項４】　請求項１ないし３のうちのいずれか１項に記載の、端末装置はメモリ中に記憶されている運用データの援助を受けて動作する伝送システムにおいて、上記防護手段は上記運用データの完全性を検出するための検出手段により形成されることを特徴とする伝送システム。

【請求項５】　請求項１ないし４のうちのいずれか１項に記載の伝送システムにおいて、上記防護手段は、真正であることが認められたときに通信を許容するための接続可能な回路を介して端末装置を認証する認証手段により形成されることを特徴とする伝送システム。

【請求項６】　請求項１ないし５のうちのいずれか１項に記載の伝送システムにおいて、上記防護手段は、端末装置と接続可能な回路との間のデータ交換を防護するための防護手段により形成されることを特徴とする伝送システム。

【請求項７】　その中に通信に関する前払いデータが入っている少なくとも１つの接続可能な回路と、上記前払いデータを通信の関数として直接変更する手段とを含むところの、通信の交換をすることのできる端末装置において、

該端末装置は前払いに関するデータの完全性を保証するための防護手段を含むことを特徴とする端末装置。

【請求項８】　請求項７に記載の、メモリ中に記憶されている運用データによりその動作が定まるところの端末装置において、上記防護手段は上記運用データの完全性を検出するための検出手段により形成されることを特徴とする端末装置。

【請求項９】　請求項７又は８に記載の端末装置において、上記防護手段は、真正であることが認められたときに通信を許容する接続可能な回路を介して端末装置を認証する認証手段により形成されることを特徴とする端末装置。

2

【請求項１０】　請求項７ないし９のうちのいずれか１項に記載の端末装置において、上記防護手段は、端末装置と接続可能な回路との間のデータ交換を防護するための防護手段により形成されることを特徴とする端末装置。

【請求項１１】　或る一定の残高を規定する前払いデータを含み、その動作はソフトウェアで規定されるところの接続可能な前払い回路が、プラグ挿入でそれに結合している複数の端末装置を有する伝送システム用の前払い方法において、該方法は次の各フェーズ、すなわち：

－　端末装置の動作ソフトウェアの完全性を確認し、また、接続可能な前払い回路のタイプを確認する開始フェーズ；

－　端末装置からのキイを接続可能な前払い回路に送出する送出フェーズ；

－　接続可能な前払い回路に含まれる残高を課金すべき最少料金と比較する接続設定フェーズ；

－　残高の内容から引き落としを行う通信中における料率課金フェーズ；を有して成ることを特徴とする前払い方法。

【請求項１２】　請求項11に記載の前払い方法において、前払いデータは周期的に或る引き落とし単位で引き落とされるものであることを特徴とする前払い方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、その中に前払いデータが入っている少なくとも１つの接続可能な回路と、通信に応じて上記前払いデータを直接変更する手段とを含むところの、通信を行うことのできる複数の端末装置を有する伝送システムに関する。

【０００２】本発明はまた、上述のシステム及びそのようなシステムに適する端末装置で実行される前払い方法にも関する。

【０００３】

【従来の技術】この種の GSM型のネットワークの基本原則は、上述のすべての装置を先ず始めに広く一般に普及させることである。それから、一般的には SIMカード又はマイクロ SIMカードと呼ばれるチップで形成される接続可能な回路を用いて、装置はユーザに対し各個人用のものにされ、該 SIMカード又はマイクロ SIMカードは、端末装置にプラグで一旦挿入されるならば、ネットワークに対しユーザを同定確認し認証することを許容する。

【０００４】ネットワーク運営者の利益のために加入者の管理を請け負う営利会社(SCS) に加入することにより SIMカードが入手できる。加入業務のみならず、 SCSはネットワーク運営者から送られて来るデータに基づいて請求業務も管理する。

【０００５】これらの管理業務は比較的高価である。それればかりでなく、財務上のリスクも無視し得ない、すなわち：若干人の加入者はその請求書に支払うことを「忘

れる、或いは怠る」のである。

【０００６】これらの理由によりネットワーク運営者及び SCSは、公衆電話ボックスで今日使われているテレフォンカードのアイディアに準じた前払いネットワークサービスの導入に関心がある。前払いタイプの SIMカードが、総ユニット数又は所定ユニット数に対応する通信を許容する。この概念は次のような種々の利点をもたらす：

－　SIMカードの配布過程の単純化；
－　加入者登録数の増加；
－　請求書発行が不要；
－　管理費用の削減；
－　進歩的な財源。

【０００７】上述のような前払いシステムはＰＣＴ特許記録第ＷＯ95/28062号から既知である。しかしこのシステムには顕著な欠点があり、それは接続可能な回路が被害を受け易いということであって、すなわち不正な策略により内容が変更されることがあり、また、この回路と端末装置との間のデータの交換が悪意のある人により盗聴されることがあり、それが不正な行動を意図する手段を提供する。

【０００８】

【発明が解決しようとする課題】本発明は、少なくとも上述の欠点を持たない冒頭に記載のタイプのシステムを提案する。

【０００９】

【課題を解決するための手段】従って冒頭に記載のタイプのシステムは、上記端末装置が前払いに関するデータの完全性を保証するための防護手段を含むことを特徴とする。

【００１０】この発明的なアイディアは、前払いデータに関するすべての情報が防護され、それによって不正を企む人が、その通信コストを誤魔化すことを実行上不可能にする、ということから成る。

【００１１】端末装置がメモリに記憶された運用データの援助を受けて機能する上述のタイプのシステムによる本発明の一態様は、上記防護手段が上記運用データの完全性を検出するための検出手段により形成されることを特徴とし、この態様は確実にそれらのデータが不正を意図する人により変更されることのないものである。

【００１２】本発明のもう１つの態様によれば、上記防護手段は、真正であることが認められたときに通信を許容するための接続可能な回路で端末装置を認証する手段により形成され、不正を企む人が他の接続可能な回路をプラグ接続して通信コストに関し彼に利益を図ろうとする可能性を回避する。

【００１３】

【実施例】以下、本発明の上記及びその他の態様が実施例及び図面により詳細に説明される。

【００１４】図１に示すシステムは、携帯形無線端末装置で１と番号を付したものを含む。この装置は GSM型の無線ネットワークの中継局８との間で電波を送受するためのアンテナ５を持っている。この装置１は、ラウドスピーカ10、マイクロフォン12、キイパッド15、及び可視ディスプレイ17を含む。破線で囲んであるのは該装置内に在る電子化部分20を表す。 GSM標準(I-ETS 300 045-1又はETS30)によれば、ISOフォーマット又はプラグインフォーマットの SIMカード、或いはマイクロ SIMカードが用意され、これは図１では30と番号が付されている。このカードはコネクタ31を持ち、それは装置１の一部を形成するもう一方の接点35と接触する。このもう一方の接点35は図２に示されている。図１のシステムには更に、装置１と同様の構造の他の装置36及び37も含まれる。

【００１５】図２には装置１の構造が更に詳細に示され、図１と図２とは同じものに同じ番号が付されている。図２は電子化部分20の構造を詳細に示す。

【００１６】この電子化部分20は GSM技術で通常用いられる種々のデータ、更に詳しく云えばマイクロフォン12から来るデータ及びラウドスピーカ10に関するデータを送受するための、送信アセンブリ40と受信アセンブリ42とを含む。マイクロプロセッサアセンブリ50が、以下の諸エレメントすなわち：送信アセンブリ40並びに受信アセンブリ42，キイパッド15，可視ディスプレイ17，及びコネクタ35並びに31を介してモジュールSIM 30とのデータ交換；の運営管理を保証する。更に詳しく云えばこのマイクロプロセッサアセンブリ50は EPROM型を好適とし、前払いデータをそれに含むことを意図する読み出し／書き込みメモリ55を有する。

【００１７】該システムは本発明によるならば SIMカードを介して通信への課金が許されるようになることが望まれている。

【００１８】従ってそのようなシステムは次の要求条件：

－　SIMカードは提供されたサービスに対応する金額だけ引き落とせる（課金計算の正確性），
－　ユーザは対応するユニットの引き落しがなされずにサービスを受けることはできない（不正使用無し），を満足させるものとする。本発明の基本原理：
－　SIMカードはユニット単位で前払いされ、残高を使い切ったとき再払い込みのできるものとできないものとがある；
－　端末装置は SIMカードの料率で課金する；
－　ネットワーク上ではカードに課金できる端末装置に SIMカードが挿入されたときにのみ SIMカードは使用できる；
－　端末装置は、端末装置のソフトウェア機能の実行を保証する信託されたプロセッサ、及び防護された環境における前払いに必要なアルゴリズムのアプリケーションを含む；

－　信託されたプロセッサは端末装置のソフトウェアの完全性を確認することができ、また変更された場合には演算動作を禁止することができる；

－　暗号プロトコルが、端末装置と SIMカード間の信託されたリンクを樹立することを許容する；

－　任意の偽造に対し暗号的に防護されている SIMカードの当初の残高が端末装置によって読み出される；

－　端末装置は SIMカードの残高の真正確実なことを保証し、また残高不足の場合には通信を禁止することができる；

－　端末装置は SIMの料率を計算する、それは通信の始めにネットワークから送られる通話料率データによるか、又はテーブルの形の予め初期化されたデータによるものとする；

－　端末装置によって SIMカードにアドレスされる料率指示は任意の偽造に対し暗号的に防護されている；

－　SIMカードの料率は、任意の偽造に対し暗号的に防護されている SIMカードの残高を介してチェックできる；

－　端末装置の信託されたプロセッサは SIMの有効な料率の暗号的確認を保証する；

－　端末装置は SIMカードの残高を使い切ったときには通信を切断する.

【００１９】図３及びそれ以後の図面は、上記要求条件を満足させるシステムの演算動作を示す図である。

【００２０】演算動作は図３及びそれ以後の図面に示されるフローチャートでそれぞれ表される４つのフェーズに分割される。これらのフローチャートは次の２つの部分すなわち：

－　端末装置１の演算動作に関するTERMと名付ける部分；及び

－　SIMカード30に関する SMCと名付ける部分；によって形成される。

【００２１】図３に示すフェーズはステップK0で始まる、このステップK0は端末装置に電源を投入するステップで、次の最初の演算は端末装置のソフトウェアの完全性を確認することから成る（ステップK2参照）。これについては本出願と同じ出願人により1996年２月７日に出願されたフランス国特許出願第 96 01 478号に記載されている。その次の試験（ステップK5）で、もしソフトウェアが侵略されていることが示されるならば、ステップK6に進んで端末装置１の停止が指示される。もしソフトウェアが無傷であるならば、 SIMカードによる端末装置の演算動作が認証されて、端末装置は通信ユニットの料率の管理ができることを保証される。これはチャレンジ／応答メカニズムによって行われる。

【００２２】この目的のために開始命令（ステップK10）が SIMカード30に与えられる。そこで該 SIMカードがスタートする（ステップL0）。該 SIMが立ち上がった後で端末装置はステップK12 で乱数の要請を SIMカードに送出する。該 SIMはその要請を受け取って乱数Asを生成することにより応答する（ステップL2）。端末装置はキイKs及び数Ｓに係わる暗号化アルゴリズムを介して働き、該アルゴリズムは SIMカードに送出される（ステップK14)。該カードは受け取った数Ｓに応答して演算を実行する。この演算はステップL4内にAg(Kv,S)と記した暗号化アルゴリズムによって規定される。もし該アルゴリズムが RSA符号化方法を含むならば２つのキイKs及びKvが用いられる。これらのキイは、もし DES方法のような対称な方法が用いられるならば、同一のものである。次にステップL6で２つの数As, As' が比較される。該比較が相違を示すならば過程は停止する（ステップL8）。カードは次回に立ち上がるまでブロックされる。

【００２３】その次のステップは伝統的にネットワークが SIMを認証するようにさせることから成る；これは、A3A8と呼ばれる(GSM標準に記載されている）アルゴリズムを使用する GSM標準の標準的手順であって、ステップL10 にはこれはAgA3A8(..)と書いてあり、該 SIMのキイKiである。もし SIMカードによる端末装置の認証が正しく終了しないならば、ネットワークによる SIMの認識の処理は実現できない、その結果、ネットワークは SIMの引き落としができないこの送受器の接続を拒絶することになろう、ということが理解されよう。従って端末装置は乱数Arをカードに送り（ステップK18)、するとカードは、上述のようにA3A8アルゴリズムの関数及びキイKiの関数として数Ｒを計算する。この数は端末装置に送出されて、更にネットワーク上に送られる（ステップK20)。中継局８のレベルでは、例えば端末装置が受容されたか拒絶されたかが判定される。

【００２４】図４に示す第２のフェーズは、端末装置と SIMカード間の交換を防護することを意図するランダムセッションキイを確立するフェーズである。端末装置はランダムセッションキイKsを生成する（ステップK30)。このキイの暗号化は、例えばRSA型のアルゴリズムで実行される（ステップK32)。キイKencが、セッションキイを生成する要請を SIMに送出するメッセージＣを求めるのに使われる（ステップK33)。 SIMカードは RSAアルゴリズムとそのキイKdecを用いてメッセージＣを復号し、求めたキイKsを記憶する。

注：－　これと同値のレイアウトが例えば DESアルゴリズムのような対称のアルゴリズムに基づいて可能である。その場合にはキイKencとキイKdecとは同一のものとなろう。

【００２５】対称アルゴリズムの実行のもう１つの変形、例えば DESアルゴリズムは、端末装置と SIMカードの既知のキイ及び現存の２つの部分により与えられる乱数を用いることから成る。端末装置は乱数Amを生成し、それを記憶して SIMカードに送出する。 SIMカードは乱数Asを生成してそれを端末装置に送出し、また

Ks-Ag(Key,As‖Am)

を計算してそれを記憶し、更にまた端末装置は論理連鎖演算を指定する。それと同時に端末装置はAsを受け取った後で更に

Ks＝Ag(Key, As‖Am)

をも計算する。

【００２６】交換局内では技巧的の程度がより少ないやり方で前以て知られている端末装置の及び SIMカードのキイKsをも用いることができる。

【００２７】第３のフェーズは、通信のパラメタを求めることを考慮に入れるフェーズであり、それはカード上のユニットの残高が確立される通信に対し十分であるか否かを確認するものである。このフェーズは図５で説明される。

【００２８】通信を開始した後で（ステップK40)通信課金料率のパラメタは、ネットワークのオペレータ又は端末装置内に前以て搭載されていたテーブルに基づいて求められる。これはステップK42 に示される。次いで方法Prd が開始され、これはすべての安全確保の保証がなされたカードの残高の回復を許容するものである。この方法は乱数Acが生成されたとき（ステップK44)に開始し、該乱数Acは残高Sld に対する要請に加えられる（ステップK46)。そうすると SIMカードは数値Acに基づく MACと呼ばれる証明書及び残高を次のやり方で計算する：

m1 ＝ Alg_D (Ac,Ks)

但し茲で、Ksは以前に確立されたセッションキイとする；

m2 ＝ Alg_D （残高（＋）m1,Ks)

但し茲で、（＋）は排他的論理和(EXCLUSIVE-OR)という演算子を表し、 Alg_D は任意のアルゴリズムを、この場合更に特定すれば DESアルゴリズムを表し、Ms ＝ MAC を形成する結果m2 の４個の最左桁バイトとなる。このことはステップL30 に表されている。次に SIMカードは乱数Adを生成し（ステップL32)、これは後に料率要請のために使われる。そして最後にカードは、Sld(残高),Ms,及び新しい乱数Adを、端末装置に送出する（ステップL33)。残高及びMs を受け取ると、端末装置はその完全性を次の再計算、すなわち：m1'＝ Alg_D (Ac,Ks)，を自分自身で確立した数値Ac及びKsに基づいて；m2'＝ Alg_D （残高（＋）m1,Ks)，を SIMの送出した残高に基づいて；再計算することによって確認する。Ms'＝m2' の４個の最左桁バイト，となる。このことはステップK48 に表されている。次いでステップK50 で、Ms'とMsとの等値が試験される。等値ならば受け取った SIMの残高の値の完全性が証明される。等値でなければその場合は通信が中断される（ステップK51)。実際にこのことは不正な意図が結果的に通信の確立を不可能にする抑止効果がある。次に（ステップK52)課金される料率Dbが、ステップK42 で受け取ったパラメタに基づいて計算される。この残高Dbと最少料率との比較（ステップK54)により、通信を確立させるか否かの判定ができる。通信が中断されるならばステップK55 に行く。通信が継続されるならばステップK56に行き、そこで変数OSLDの割当てが指示される。この変数はカードから来る残高の数値を含むようにしてある。端末装置は SIMから受け取った乱数Adを記憶し、次回の料率要請に同じく利用する。

【００２９】第４のフェーズのフローチャートは図６に示され、これは通信中にカードに課金される料率を示す。このフェーズは或る課金料率が課金されようとする瞬間にスタートする（ステップK60)。この開始は、例えば周期的に料率ユニットDbの課金をさせようとする端末装置によってなされる。課金演算はステップK62 で説明される証明書（１つのMAC)によって防護されている。次いで料率に対する要請がSIMカードに送られる（ステップK64)。そこでは、選定されたキイKs（ステップL50)に基づいて証明書Md'が定められ（ステップL51)、それが端末装置から送出された証明書Md と比較される（ステップL55)。比較の結果が良好ならばステップL60 に進み、そこで新しい残高の演算動作が指示される。この新しい残高がプラスの数であることを確認するのは適切であり、それはステップL62 で実行される。もし残高がマイナスの数ならばカードはブロックされる（ステップL63)。もし残高がプラスの数ならば何らの演算も行われない。該カードはＯＫと宣言されて（ステップL65)、それは端末装置に送出される。

【００３０】そうすると端末装置は、この宣言（ステップK65)を試験することにより該 SIMカードが有効であるか否かを確認することが可能である。もし SIMカードがブロックされているならば、ＯＫと宣言されていないので、通信は停止する（ステップK66)。もし SIMカードが有効ならば方法Prd を実行することにより過程は継続されて、残高値の回復が許容される。真の料率の確認が実行され（ステップK70)変数OSLDはステップK75 で更新される。確認が料率の実施されていないことを示すならば通信は停止する（ステップK71)。

【００３１】本発明は GSM型のネットワーク以外の分野、特に電話ネットワーク、DCS 1800タイプのデータ伝送ネットワーク、車載又は固定電話端末装置（公衆電話機）、ファクシミリ、データ又は画像伝送端末装置、等々にも適用領域が見出され、また防護も監視もされていない環境で使用される端末装置にも適用されよう。

【図面の簡単な説明】

【図１】図１は、本発明によるシステムを示す図である。

【図２】図２は、図１に示すシステムに適する携帯形無線端末装置を示す図である。

【図３】図３は、本発明によるシステムの演算動作を説明することを意図した第１のフローチャートを示す図である。

【図４】図４は、本発明によるシステムの演算動作を説明することを意図した第２のフローチャートを示す図で

ある。

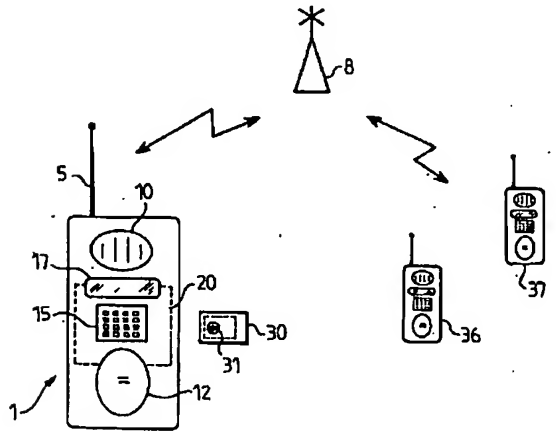
【図５】図５は、本発明によるシステムの演算動作を説明することを意図した第３のフローチャートを示す図である。

【図６】図６は、本発明によるシステムの演算動作を説明することを意図した第４のフローチャートを示す図である。

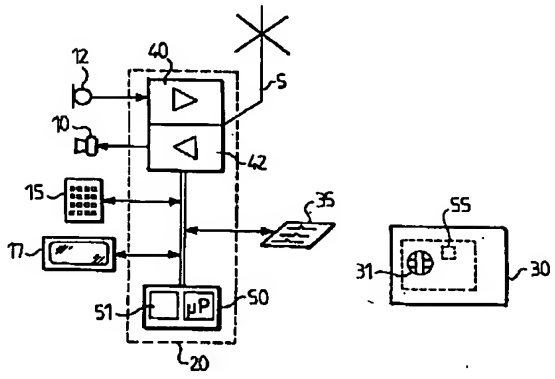
【符号の説明】

1　携帯形無線端末装置
5　アンテナ
8　無線ネットワークの中継局
＊10　ラウドスピーカ
12　マイクロフォン
15　キイパッド
17　可視ディスプレイ
20　携帯形無線端末装置内の電子化部分
30　SIMカード
40　送信アセンブリ
42　受信アセンブリ
50　マイクロプロセッサアセンブリ
55　読み出し／書き込みメモリ

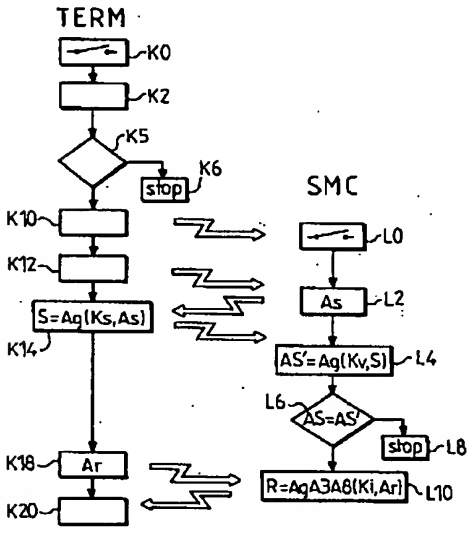
【図１】



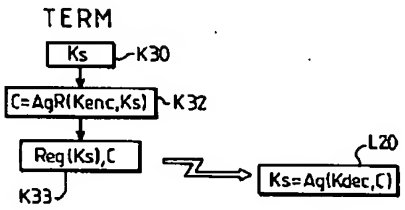
【図２】



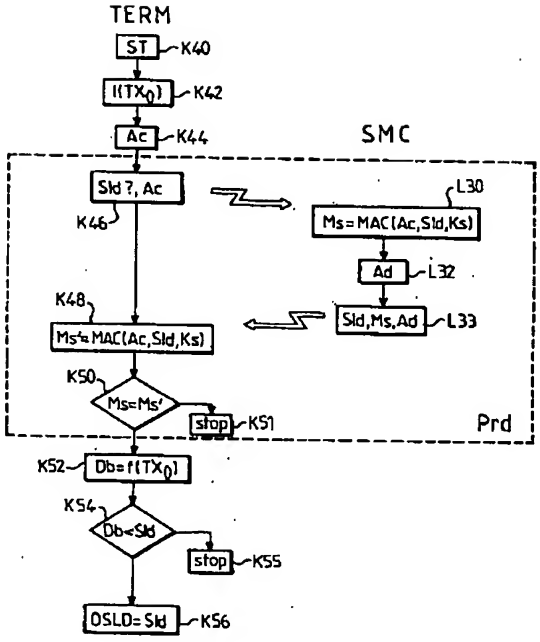
【図３】



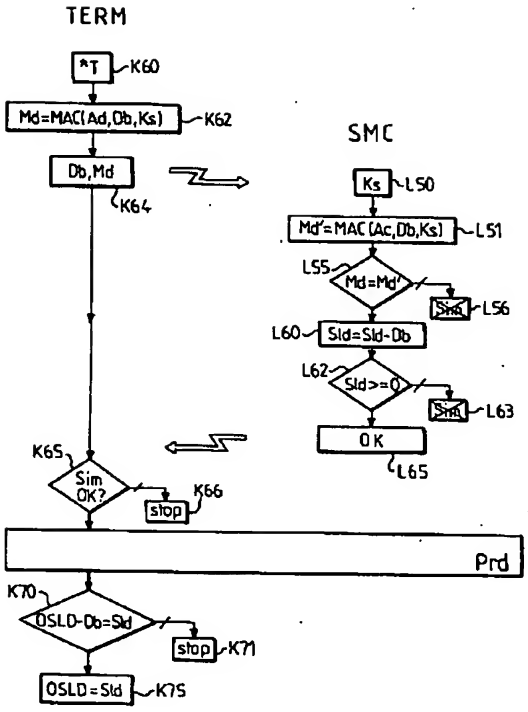
【図４】



【図５】



【図６】



【手続補正書】
【提出日】平成９年３月２１日
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】請求項３
【補正方法】変更
【補正内容】
【請求項３】　請求項１に記載の伝送システムにおいて、課金料率データは各端末装置のレベルで接続可能な回路内に含まれているテーブルによって定められることを特徴とする伝送システム。